ABELIAN VARIETIES DEFINED OVER THEIR FIELDS OF MODULI, I†

J. S. MILNE

Whenever we consider a triple $(A, \mathscr{C}, \theta)$ we will mean that A is an abelian variety of dimension d, $\mathscr{C}$ is a polarization of A, $\theta : F \to \mathrm{End}^\circ(A) = \mathrm{End}\,(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ is a ring homomorphism where F is a field of degree $2d$ over $\mathbf{Q}$, $\theta(F)' = \theta(F)$ where $\alpha \mapsto \alpha'$ is the involution of $\mathrm{End}^\circ(A)$ induced by $\mathscr{C}$, and that A, $\mathscr{C}$, and θ are all defined over some subfield of the complex numbers $\mathbf{C}$. F is then necessarily a CM-field, and $(A, \mathscr{C}, \theta)$ is of type $(F, \Phi; \mathfrak{a}, \zeta)$ in the sense of [5, p. 128] for some lattice $\mathfrak{a}$ in F and element ζ of F. We will assume that the reader is familiar with the definitions in [5].

Our main result is that $(A, \mathscr{C}, \theta)$ always has a model defined over its field of moduli k_0, i.e. that there is an $(A_0, \mathscr{C}_0, \theta_0)$ defined over k_0 which becomes isomorphic to $(A, \mathscr{C}, \theta)$ over $\mathbf{C}$. As a consequence, one gets an alternative proof of a theorem of Casselman's [6, Theorem 6] characterizing those Grössen-characters which arise from abelian varieties. Also, one obtains a positive answer to a question of Shimura's concerning the existence of such Grössen-characters [6, p. 513].

In a second paper we intend to consider the question of, given $(A, \mathscr{C}, \theta)$, when is the pair $(A, \mathscr{C})$ defined over its field of moduli.

We write k_{ab} for the maximal abelian extension of a field k, and $\bar{k}$ for its algebraic closure. (F', Φ') denotes the reflex of a CM-type (F, Φ).

THEOREM. *Let $(A, \mathscr{C}, \theta)$, as above, be of CM-type (F, Φ). Then there is a model $(A_0, \mathscr{C}_0, \theta_0)$ of $(A, \mathscr{C}, \theta)$ defined over the field of moduli k_0 of $(A, \mathscr{C}, \theta)$ and such that all torsion points of A_0 are rational over F'_{ab}.*

Proof. Let S be the (ordered) set of points of A of order 3, and let k_1 be the field of moduli of $(A, \mathscr{C}, \theta, S)$.

(i) $F' \subset k_1 \subset F_{ab}$
This follows from [5, 5.16]

(ii) There is a model $(A_1, \mathscr{C}_1, \theta_1, S)$ for $(A, \mathscr{C}, \theta, S)$ defined over k_1.
It is easy to see that there is a finite normal extension K of k_1 such that $(A, \mathscr{C}, \theta, S)$ is defined over K and such that for every $\sigma \in \mathrm{Gal}\,(K/k_1)$ there is an isomorphism $\lambda_\sigma : (A, \mathscr{C}, \theta, S) \to (A^\sigma, \mathscr{C}^\sigma, \theta^\sigma, S^\sigma)$ defined over K. Let $\lambda_{\tau,\sigma} = \lambda^\sigma_{\sigma^{-1}\tau}$ for $\sigma, \tau \in \mathrm{Gal}(K/k_1)$. From the fact that $\mathrm{Aut}\,(A, \mathscr{C}, \theta, S) = \{1\}$ [3, §21, Thm 5] it follows that

$$\lambda^\rho_{\tau,\sigma} = \lambda_{\rho\tau,\rho\sigma}$$

$$\lambda_{\tau,\sigma}\lambda_{\sigma,\rho} = \lambda_{\tau,\rho}$$

Received 8 June, 1972.

†This paper was written while the author was a visitor at King's College, London and the University of Nottingham, and was supported by the Science Research Council.

for all ρ, σ, $\tau \in \mathrm{Gal}(K/k_1)$. Assertion (ii) now follows from [7].

(iii) A_1, as in (ii) above, has all of its torsion points rational over F'_{ab}
This is [5, 7.8.8].

Regard now $(A, \mathscr{C}, \theta)$ as being defined over k_1 and satisfying (iii). If $k_1 = k_0$ then the theorem is proved. If not, there is a field k_2, $k_1 \supset k_2 \supset k_0 \supset F'$, such that k_1/k_2 is Galois of prime degree p (use (i)). Let σ generate $\mathrm{Gal}(k_1/k_2)$ and let $\lambda : (A, C, \theta) \to (A^\sigma, C^\sigma, \theta^\sigma)$ be an isomorphism.

(iv) λ is defined over k_1.
This is a consequence of [6, Thm 5, Pptn 1]. Alternatively it may be proved as follows. $a \mapsto a^\sigma$ is an isomorphism $V_l A \to V_l A^\sigma$ which commutes with the actions of F and of $\mathrm{Gal}(\bar{k}_1/k_1)$ (use (iii)). But it is clear from [4, Cor 2 to Thm 5] that any homomorphism $V_l A \to V_l A$ which commutes with the action of F commutes with the action of $\mathrm{Gal}(\bar{k}_1/k_1)$. Thus $\lambda^\tau = \lambda$ for all $\tau \in \mathrm{Gal}(\bar{k}_1/k_1)$ which proves (iv).

Write ν for the canonical isomorphism
$(a^{\sigma^p} \mapsto a) : (A^{\sigma^p}, \mathscr{C}^{\sigma^p}, \theta^{\sigma^p}) \to (A, \mathscr{C}, \theta)$. Then $\Lambda = \nu\lambda^{\sigma^{p-1}} \dots \lambda^\sigma \lambda$ is an automorphism of $(A, \mathscr{C}, \theta)$, and hence may be written as $\theta(\alpha)$ with $\alpha \in \mu(R)$ where $R = \theta^{-1}(\mathrm{End}_{\mathbf{C}}(A))$ and $\mu(R)$ is the set of roots of unity in R.

(v) α is a pth power in R.
If μ is a homomorphism of abelian varieties we write μ_l for the corresponding map on the Tate groups T_l (or V_l). The map $a \mapsto \lambda_l^{-1}(a^\sigma) : T_l A \to T_l A$ is $\mathbf{Z}_l$-linear and commutes with the action of $\theta(R)$. By [4, Cor. 1 to Thm. 5] there exists an $\alpha_l \in R_l = R \otimes_{\mathbf{Z}} \mathbf{Z}_l$ such that $\lambda_l^{-1}(a^\sigma) = \theta(\alpha_l^{-1})(a)$ all $a \in T_l A$. It follows that $\Lambda_l(a) = \theta(\alpha_l^p)(a)$ all $a \in T_l A$. Hence $\theta(\alpha) = \theta(\alpha_l^p)$, and so α is a pth power in R_l for all primes l. By class field theory, e.g. [1, X], this implies that α is a pth power in F, say $\alpha = \beta^p$. By using that $\alpha \in \mu(R)$ and is a pth power in R_l for all l, one gets that $\beta \in R_l$ for all l. But $R = \bigcap R_l$, and so $\beta \in R$.

Replace λ by $\lambda\theta(\beta^{-1})$, so that now $\Lambda = 1$. Define $\lambda_{j,i} : A^{\sigma^i} \to A^{\sigma^j}$ by

$$\lambda_{j,i} = \lambda^{\sigma^{j-1}} \dots \lambda^{\sigma^i},$$

$0 \leqslant i \leqslant j \leqslant p-1$, and $\lambda_{j,i} = \nu^{\sigma^j} \lambda_{j+p,i}$, $0 \leqslant j \leqslant i \leqslant p-1$. Then $\lambda_{k,j}\lambda_{j,i} = \lambda_{k,i}$ and $\lambda_{j,i}^\sigma = \lambda_{j+1\ i+1}$ and so [7] there is an $(A_2, \mathscr{C}_2, \theta_2)$ defined over k_2 which is isomorphic to $(A, \mathscr{C}, \theta)$ over k_1. Note that A_2 will therefore also satisfy (iii). If $k_2 = k$ the proof is complete. If not, the above process may be used to find an $(A_3, \mathscr{C}_3, \theta_3)$ over some k_3, $k_2 \supset k_3 \supset k$, $k_2 \neq k_3$. By continuing in this way, one eventually obtains the desired result.

In order to state the two corollaries, consider $(A, \mathscr{C}, \theta)$ defined over some number field k, and let it be of type $(F, \Phi; \mathfrak{a}, \zeta)$. Regard F as a subfield of $\mathbf{C}$, write I_k for the idèle group of k, put $I_{k,\infty} = k \otimes_{\mathbf{Q}} \mathbf{R} \subset I_k$, and write $I_k{}^\infty$ for the group of finite idèles of k, i.e. those whose component at any infinite prime is 1. If $x \in I_F$, write x_1 for the component of x corresponding to the infinite prime defined by the given embedding of $F \subset \mathbf{C}$. Then $\det \Phi'$ defines a homomorphism $F'^* \to F^*$ and, since $k \supset F'$, we get a homomorphism $g = (\det \Phi') N_{k/F'} : k^* \to F^*$. This extends to a continuous homomorphism $I_k \to I_F$ which we also denote by g.

As explained in [6, p. 510], one obtains from $(A, \mathscr{C}, \theta)$ a Grössen-character $\psi : I_k \to \mathbf{C}^*$ such that,

(1) for all $x \in I_{k,\infty}$, $\psi(x) = g(x)_1^{-1}$, and

(2) for all $x \in I_k^{\infty}$, $\psi(x) \in F^*$, $\psi(x)\overline{\psi(x)} = |x|_0$, and $\psi(x)\,\mathfrak{a} = g(x)\,\mathfrak{a}$, where $\overline{\psi(x)}$ is the complex conjugate of $\psi(x)$ and $|x|_0$ is the absolute norm of the ideal associated to x. Conversely, there is the following result.

COROLLARY 1. *Let k be a finite extension of F'. Any Grössen-character $\psi : I_k \to \mathbf{C}^*$ satisfying* (1) *and* (2) *arises from some $(A, \mathscr{C}, \theta)$ of type $(F, \Phi; \mathfrak{a}, \zeta)$ defined over k.*

Proof. Let $(A, \mathscr{C}, \theta)$ be any structure of type $(F, \Phi; \mathfrak{a}, \zeta)$. It follows from [5, 5.16] that k contains the field of moduli of $(A, \mathscr{C}, \theta)$ and so we may take $(A, \mathscr{C}, \theta)$ to be defined over k. Let ψ' be the Grössen-character arising from $(A, \mathscr{C}, \theta)$ and put $\chi = \psi/\psi'$. By (1), χ is a Dirichlet character and so may be regarded as a character of $G = \mathrm{Gal}\,(K/k)$ for some finite abelian extension K of k. Let R_χ be R regarded as a G-module by defining $\sigma\alpha = \chi(\sigma)\,\alpha$ for $\sigma \in G$, $\alpha \in R$. Then, in the notation of [2, §2], $(A', \mathscr{C}', \theta')$ with $A' = R_\chi \otimes_R A$ and obvious θ' and $\mathscr{C}'$ is of type $(F, \Phi; \mathfrak{a}, \zeta)$ and has Grössen-character $\chi\psi' = \psi$.

COROLLARY 2. *Let k be a finite extension of* $\mathbf{Q}$ *and let $(F, \Phi; \mathfrak{a}, \zeta)$ be a possible type for a structure $(A, \mathscr{C}, \theta)$. Then there is a Grössen-character $\psi : I_k \to \mathbf{C}^*$ satisfying* (1) *and* (2) *if and only if k contains the field of moduli of some $(A, \mathscr{C}, \theta)$ of type $(F, \Phi; \mathfrak{a}, \zeta)$.*

Proof. The necessity follows from [5, 5.16] and the sufficiency from the theorem.

Remarks 1. In [6], Corollary 1 is proved directly and then, under certain hypotheses on R ((5.2) loc. cit.), Shimura explicitly constructs a Grössen-character ψ satisfying (1) and (2) and so deduces a weaker form of our Theorem 1.

2. Given A and the map θ it is always possible to find a polarization $\mathscr{C}$ such that $\theta(F)' = \theta(F)$ [5, p. 128]. Moreover [6, Pptn 4] the field of moduli of $(A, \mathscr{C}, \theta)$ is independent of the $\mathscr{C}$ chosen. Thus it makes sense to speak of the field of moduli of (A, θ), and then Theorem 1 implies that this is also the smallest field of definition of (A, θ).

References

1. E. Artin and J. Tate, *Class field theory* (Harvard University, 1961).
2. J. Milne, " On the arithmetic of abelian varieties ', *Inventiones math.* (to appear).
3. D. Mumford, *Abelian varieties* (Oxford University Press, London, 1970).
4. J.-P. Serre and J. Tate, " Good reduction of abelian varieties ", *Ann. of Math.*, 88 (1968), 492–517.
5. G. Shimura, *Introduction to the arithmetic theory of automorphic functions* (Princeton U.P. 1971).
6. ———, " On the zeta-function of an abelian variety with complex multiplication ", *Ann. of Math.*, 94 (1971), 504–533.
7. A. Weil, " The field of definition of a variety ", *Amer. J. Math.*, 78 (1956), 509–524.

University of Michigan.